

AMENDED CLAIMS

[received by the International Bureau on 28 October 2004 (28.10.2004);
original claim 10 amended;
remaining claims unchanged (2 pages)]

the watermark insertion apparatus according to
claim 1;

a program input section that inputs a program in
which the watermark insertion apparatus according to
5 claim 1 has inserted said watermark and said watermark
verification code; and

a watermark detection section that extracts said
watermark from said program and generates ID information
that uniquely identifies said distribution destination
10 based on said watermark;

wherein a distribution destination is identified
based on generated said ID information.

8. The program illegal distribution prevention system
15 according to claim 7, wherein said watermark insertion
apparatus is provided at said distribution destination.

9. A watermark insertion method wherein:

watermark that differs for each program
20 distribution destination is inserted in said program and
said watermark is used;

said program is prevented from operating correctly
when said watermark is tampered with; and

watermark verification code that is identical
25 regardless of said distribution destination is inserted
in said program.

10. (Revised) A watermark insertion method comprising:

inserting a in a program watermark that differs for each program distribution destination; and
converting a part other than a location at which said watermark is inserted while maintaining
5 specifications of said program.

11. A watermark insertion program that causes a computer to:

insert watermark that differs for each program
10 distribution destination in said program and use said watermark;

prevent said program for distribution from operating correctly when said watermark is tampered with;
and

15 insert watermark verification code that is identical regardless of said distribution destination in said program for distribution.

12. A watermark insertion apparatus comprising:

20 a watermark insertion section that inserts in a program watermark that differs for each program distribution destination; and

a conversion section that converts a part other than a location at which said watermark is inserted while
25 maintaining specifications of said program.

13. The watermark insertion apparatus according to claim 12, wherein said conversion section inserts an

Statement under PCT Article 19(1)

As generally recited in claim 1 of the present application, the present invention has a feature of inserting into a program watermark verification code that prevents the program from operating correctly when watermark information is tampered with. In particular, claim 1 recites a feature of making the watermark verification code identical regardless of the distribution destination.

By this means, when programs in which watermark information and watermark verification code are inserted by the same method are subjected to a collusion attack, it is difficult to identify the verification code inserted in these programs.

As a result, even when the location of an electronic watermark inserted in a program is identified by the above collusion attack and this portion is tampered with, it is not possible identify the verification code inserted and operate the program accurately.

The present invention thus prevents tampering of electronic watermarks by collusion attack.

By contrast with the present invention, the COLLBERG reference discloses a method that embeds a unique identification number as watermark, per distribution destination. In addition, when an electronic watermark is tampered with, the method detects the tampering and adds tamper-proofing code that prevents the execution

of the program.

In other words, the method of the COLLBERG reference inserts tamper-proofing code, which is equivalent to the verification code of the present invention.

5 In addition, as generally recited in claim 10 of the present application, the present invention obfuscates other portions than where an electronic watermark is inserted in a program and thereby makes it difficult to identify the location in the program where the electronic
10 watermark is inserted even when programs for different distribution destinations are compared. By this means, it is possible to prevent tampering of electronic watermarks by collusion attack on programs.

By contrast with the above-noted feature of the
15 present invention, the PALSBERG reference discloses a method that obfuscates code for generating electronic watermarks and a program with an electronic watermark including code for generating electronic watermarks, and thereby makes it difficult to specify the code for
20 generating electronic watermarks and prevents tampering of electronic watermarks.